HP Select Identity Software

Connector for Citrix Password Manager

Connector Version: 1.12

Installation and Configuration Guide

Document Release Date: September 2007
Software Release Date: September 2007

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Select Identity uses software from the Apache Jakarta Project including:

- Commons-beanutils
- Commons-collections
- Commons-logging
- Commons-digester
- Commons-httpclient
- Element Construction Set (ecs)
- Jakarta-poi
- Jakarta-regexp
- Logging Services (log4j)

Additional third party software used by Select Identity includes:

- JasperReports developed by SourceForge
- iText (for JasperReports) developed by SourceForge
- BeanShell
- Xalan from the Apache XML Project
- Xerces from the Apache XML Project
- Java API for XML Processing from the Apache XML Project
- SOAP developed by the Apache Software Foundation
- JavaMail from SUN Reference Implementation
- Java Secure Socket Extension (JSSE) from SUN Reference Implementation
- Java Cryptography Extension (JCE) from SUN Reference Implementation
- JavaBeans Activation Framework (JAF) from SUN Reference Implementation

- OpenSPML Toolkit from OpenSPML.org
- JGraph developed by JGraph
- Hibernate from Hibernate.org
- BouncyCastle engine for keystore management, bouncycastle.org

This product includes software developed by Teodor Danciu (http://jasperreports.sourceforge.net). Portions Copyright © 2001-2004 Teodor Danciu (teodord@users.sourceforge.net). All rights reserved.

Portions Copyright © 1994-2004 Sun Microsystems, Inc. All Rights Reserved.

This product includes software developed by the Waveset Technologies, Inc. (www.waveset.com). Portions Copyright © 2003 Waveset Technologies, Inc. 6034 West Courtyard Drive, Suite 210, Austin, Texas 78730. All rights reserved.

Portions Copyright © 2001-2004, Gaudenz Alder. All rights reserved.

Trademark Notices

AMD and the AMD logo are trademarks of Advanced Micro Devices, Inc.

Intel and Pentium are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

JAVA™ is a US trademark of Sun Microsystems, Inc.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California

UNIX® is a registered trademark of The Open Group.

Support

You can visit the HP software support web site at:

http://www.hp.com/go/hpsoftwaresupport

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require an active support contract.

To find more information about support access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1 Documentation Map

This chapter describes the organization of HP Select Identity connector documentation and provides necessary information on how to use the documentation set to install and configure the connectors.

Figure 1 illustrates the documentation map for HP Select Identity connector. For a list of available product documentation, refer to the Table 1.

Figure 1 Documentation Map

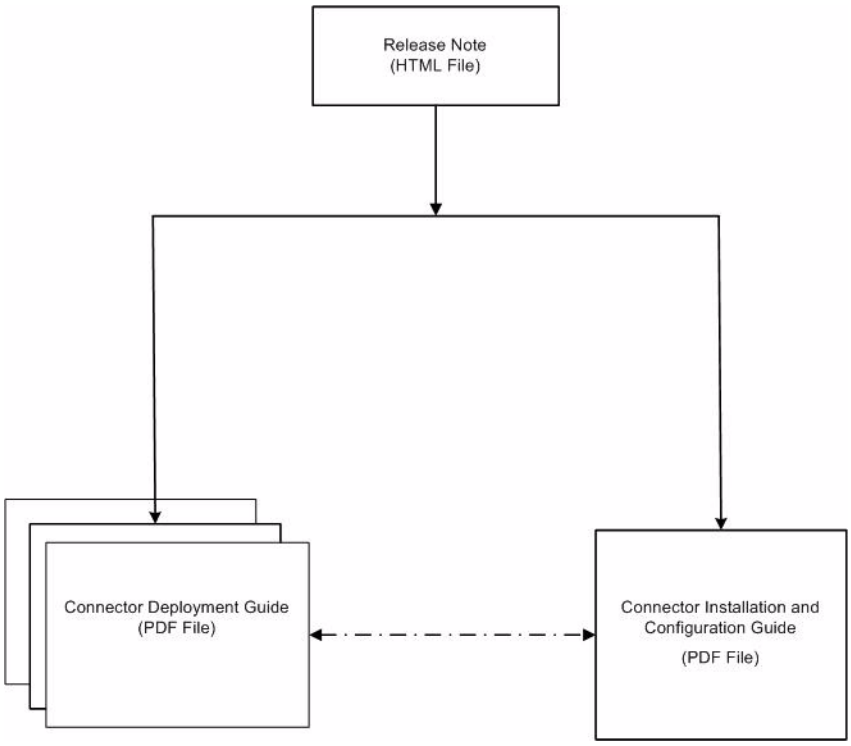


Table 1 Connector Documentation

Document Title and Filename	Contents	Location
Release Note `Citrix Connector v1.1 Release Note.htm`	This file contains necessary information on new features of the connector, enhancements, known problems or limitations, and support information.	`/Docs/` subdirectory under the connector directory.
Connector Deployment Guide (for Select Identity 4.20) `connector_deploy_SI4.20.pdf`	Connector deployment guides provide detailed information on: • Deploying a connector on an application server. • Configuring a connector with Select Identity. Refer to these guides when you need generic information on connector installation.	`/Docs/` root directory on the product's CD media.
Connector Deployment Guide (for Select Identity 4.10-4.13) `connector_deploy_SI4.13.pdf`		
Connector Deployment Guide (for Select Identity 4.0-4.01) `connector_deploy_SI4.pdf`		
Connector Deployment Guide (for Select Identity 3.3.1) `connector_deploy_SI3.3.1.pdf`		
Connector Installation and Configuration Guide `Citrix_guide.pdf`	Connector installation and configuration guide provides installation instructions for a specific connector. It contains resource specific configuration details.	`/Docs/` subdirectory under the connector directory.

2 Introduction

This chapter gives an overview of the HP Select Identity connector for Citrix Password Manager. An HP Select Identity connector for Citrix Password Manager enables you to provision users and manage identities on Citrix Password Manager system. At the end of this chapter, you will be able to know about:

- The benefits of HP Select Identity.
- The role of a connector.
- The connector for Citrix Password Manager.

About HP Select Identity

HP Select Identity provides a new approach to identity management. Select Identity helps you automate the process of provisioning and managing user accounts and access privileges across platforms, applications, and corporate boundaries. Select Identity communicates with the enterprise information system through connectors, and automates the tasks of identity management. The enterprise information system, which is also referred to as **resource**, can be a database, a directory service, or an ERP package, among many others.

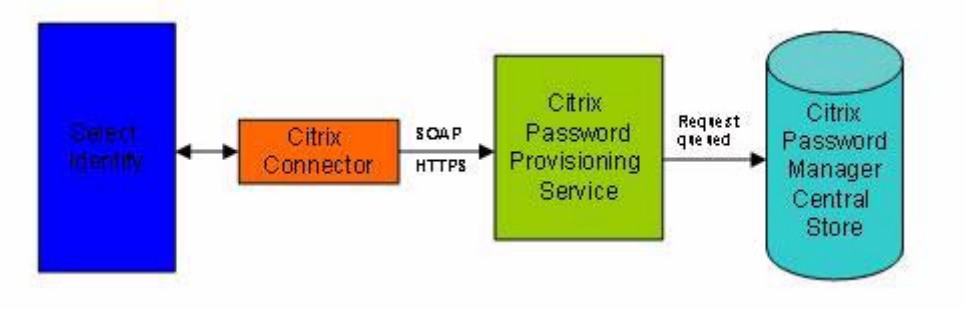
About Connectors

You can establish a connection between a resource and Select Identity by using a connector. A connector is resource specific. The combination of Select Identity and connector helps you perform a set of tasks on the resource to manage identity. A connector can be **unidirectional** or **bidirectional**. A unidirectional connector helps you manage identities from Select Identity, but if any change takes place in resource, it cannot communicate that back to Select Identity. On the other hand, a bidirectional connector can reflect the changes made on resource back to Select Identity. This property of bidirectional connectors is known as **reverse synchronization**.

About Citrix Password Manager Connector

The connector for Citrix Password Manager — hereafter referred to as Citrix connector — enables Select Identity to perform provisioning tasks on Citrix Password Manager. The connector communicates to the Citrix Password Provisioning Web Service by exchanging SPML payloads. The connector provisions Secondary Credentials to Citrix Password Manager. The communication model of Citrix connector is illustrated in the diagram below.

Figure 2 Communication Model of Citrix Connector



The Citrix connector enables you to perform the following tasks on Citrix Password Manager system by using Select Identity.

- Add, update, and remove Secondary Credentials for users.
- Retrieve Credential details for a User.
- Verify existence of credential for a User.
- Change user's credential passwords.
- Reset user's credential passwords.

It is a unidirectional connector and pushes changes made to user data in the Select Identity database to a target Citrix Password Manager and its configured user store (such as Active Directory or NTFS File Share).

This connector can be used with Select Identity version 3.3.1-4.20.

Overview of Installation Tasks

Before you start installing the connector, you must ensure that system requirements (hardware and software) and all the installation prerequisites are met. Refer to the Table 2 for an overview of installation tasks.

Table 2 Organization of Tasks

Task Number	Task Name	Reference
1	Install the connector on the Select Identity server.	See Installing the Connector on page 13.
	— Meet the system requirements.	See System Requirements on page 13.
	— Extract contents of the Schema file (file that contains the mapping files for the connector) to location on the Select Identity server.	See Extracting Contents of the Schema File on page 15.
	— Install the Resource Adapter Archive (RAR) of the connector on an application server.	See Installing the Connector on page 13.
2	Configure the connector with the Select Identity server.	See Configuring the Connector with Select Identity on page 17.

3 Installing the Connector

This chapter elaborates the procedure to install Citrix connector on Select Identity server. At the end of this chapter, you will know about

- Software requirements to install the Citrix connector.
- Prerequisite conditions to install Citrix connector.
- Procedure to install Citrix connector.

Citrix Connector Files

Citrix connector is packaged with the following files.

Table 3 Citrix Connector Files

Serial Number	File Name	Description
1	• `CitrixConnector_420.rar` for WebSphere • `CitrixConnector_420WL9.rar` for WebLogic	The connector RAR file (the binaries).
2	`CitrixConnectorSchema.jar`	It contains the Citrix Schema Mapping file.

These files are located in the `Citrix` directory on the Select Identity Connector CD.

System Requirements

The Citrix connector is supported in the following environment:

Table 4 Platform Matrix for Citrix connector

Select Identity Version	Application Server	Database
3.3.1	Weblogic 8.1.4 on Windows 2003.	Microsoft SQL Server 2000
	Weblogic 8.1.4 on HP-UX 11i.	Microsoft SQL Server 2000
4.0-4.20	The Citrix connector is supported on all the platform configurations of Select Identity 4.0-4.20.	

This connector is supported with Citrix Password Manager, version 4.1, on Windows 2003.

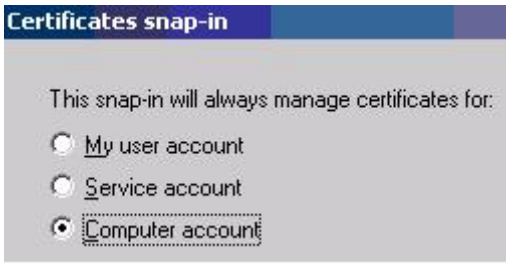
Pre-Installation Task

Before configuring the Citrix connector on Select Identity, you must set up the SSL Truststore on the Select Identity machine by extracting the CA root certificate from Citrix installation because the connector uses SSL Truststore to connect to the Citrix Password Provisioning Web Service of Citrix Password Manager.

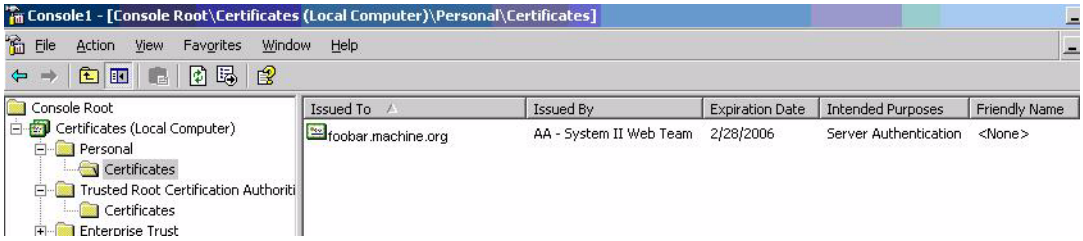
Set up the Secure Socket Layer (SSL) Truststore

Perform the steps below to obtain the CA root certificate and create SSL Truststore.

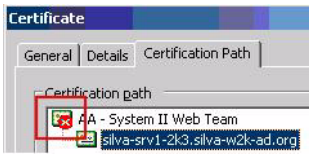
1. On the Citrix Password Manager server, go to **Start** → **Run: mmc**
2. Select **Add/Remove Snap-in** → **Add Certificates.**
3. Select the Computer Account radio button and click **Next**.
4. Click **Finish**, and then **OK**.



5. In the Console root, expand **Certificates** → **Personal** → **Certificates.**
6. Machine's new certificate appears on right pane. The Fully Qualified Domain Name (FQDN) of the machine appears in Issued To column. The certificate authority (For example, AA - System II Web Team) appears in Issued By column.

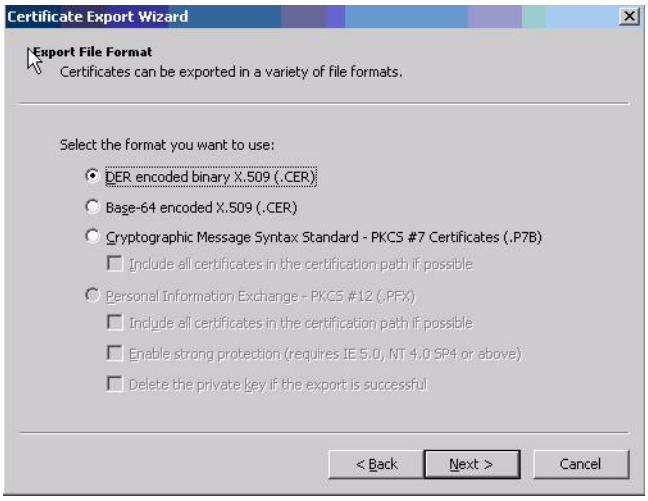


7. Double click on **Server** Certificate, choose the Certification Path tab, double click the topmost certificate (the Root CA) - the one highlighted with red X.



The root CA certificate appears

8 Choose the Details tab of this certificate, click **Copy to File**, and then export the DER encoded certificate to a local directory.



9 After you extract the certificate into a file, you must store it (this contains the CA certificate of the Root CA of Citrix Provisioning service's server certificate) to Select Identity machine at `<BEA_JAVA_HOME>\jre\lib\security`. This is the truststore used by Citrix Connector during SSL handshake with Citrix provisioning service.

10 To import the certificate, run the Java keytool command from `<BEA_JAVA_HOME>\bin` as:
`keytool -import -file CARootCert.cer -keystore cacerts`
The password for default cacerts Truststore is: `changeit`
When prompted for `Trust this certificate? [no]:` , enter **`yes`**.

11 If the application server is still running, you must restart it for the import to take effect.

Extracting Contents of the Schema File

The Schema file of the connector contains necessary mapping information to map resource attributes to Select Identity. Extract contents of the `CitrixConnectorSchema.jar` file to a directory that is in the application server `CLASSPATH`. Refer to the *HP Select Identity Connector Deployment Guide* for detailed instruction to extract contents of the Schema file.

Installing the Connector RAR

To install the RAR file of the connector (such as `CitrixConnector_420.rar`) on the Select Identity server, you must copy the file to a local subdirectory on the Select Identity server, and then deploy on the application server. Refer to the *HP Select Identity Connector Deployment Guide* for detailed information on deploying a RAR file on an application server.

While deploying the RAR on WebSphere, enter the JNDI Pool Name as **`eis/CitrixConnector`**.

After deploying the connector RAR on application server, you must configure Citrix connector with Select Identity. Refer to Configuring the Connector with Select Identity on page 17 for configuration steps.

4 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the Citrix connector with Select Identity and the connector specific parameters that you must provide while configuring the connector with Select Identity.

Configuration Procedure

After you deploy the connector RAR on application server, you must configure the connector with Select Identity. Perform the following steps to configure the Citrix connector with Select Identity.

1 Add a New Connector

2 Add a New Resource

3 Map Attributes

Add a New Connector

Add a new connector in Select Identity by using the user interface. While adding the connector, do the following:

- In the Connector Name text box, specify a name for the connector.
- In the Pool Name text box, enter **`eis/CitrixConnector`**.
- Select No for the Mapper Available section.

Refer to the *HP Select Identity Connector Deployment Guide* for detailed information on adding a new connector in Select Identity.

Add a New Resource

Add a new resource in Select Identity that uses the newly added connector. Refer to the *HP Select Identity Connector Deployment Guide* for detailed instructions on adding a resource in Select Identity.

Refer to the following table while entering the parameters in the Basic Information and the Access Information pages:

Table 5 Resource Configuration Parameters

Field Name	Sample Values	Description	Comment
Resource Name	Citrix	Name given to the resource.	
Connector Name	Citrix	The newly deployed connector.	On Select Identity 3.3.1, this field is known as Resource Type.
Authoritative Source*	No	Whether this resource is a system that is considered to be the authoritative source for user data in your environment. You must specify No because the connector cannot synchronize account data with the Select Identity server.	
Associate to Group		Whether the system uses the concept of groups. For this connector, select this option.	This is applicable only for Select Identity 3.3.1.
Citrix Password Provisioning Service Endpoint URL	**https://<CitrixHostFullName>/MPMService/ProvisionSvc.asmx**	The Endpoint URL of the Citrix Password Provisioning Service. This service maybe installed on the same machine as Citrix Password Manager or different machine.	

Table 5 Resource Configuration Parameters (cont'd)

Field Name	Sample Values	Description	Comment
Application Name	ApplicationName	The Application Definition Name of the application to which credentials are to be provisioned. This should be exactly the same value (case sensitive) as that of the Application Definition name. Refer the Access Console Suite of Citrix Password Manager or consult Citrix Administrator for obtaining the Application Definition name.	
User Name	Administrator	The username with READ+WRITE access to the Citrix Password Manager central store (Active Directory/NTFS File Share).	
Password	password	Password of the user with READ+WRITE access to central store.	
Domain Name	Citrixtest	The Domain name under which the Citrix Password Manager machine is present in.	
Schema Mapping File	`CitrixSchemaMapping.xml`	The Schema Mapping XML file name for Citrix Connector.	

Map Attributes

After successfully adding a resource for the Citrix connector, you must map the resource attributes to Select Identity attributes. Refer to the *HP Select Identity Connector Deployment Guide* for information on mapping and creating attributes. While mapping attributes, refer to the following table for resource specific mapping information.

Table 6 Citrix Mapping Information

Select Identity Resource Attribute	Citrix Password Manager Attribute	Description
UserFQDN*	userFQDN	The Fully-Qualified-Domain-Name of the User to whom credentials are to be provisioned for the Application Definition part of Resource Creation parameters (Application Name). This can be of format '<Domainname>\<Username>' or 'CN=sid2000,CN=Users,DC=citrixtest,DC=com'.
CredentialName	CredentialName	The name of the Secondary Credential to be provisioned. This is optional. If the value is not provided, the Application Name (in the Connection Parameters) is taken as the default CredentialName.
CredentialDescription	description	The description of the secondary credential.
ProvisionDescription	provision-description	This is Administrator data that is not viewable or editable by the Agent. This is provided solely for the convenience of the Provisioning Administrator
CitrixGUID*	CitrixGUID	This is a unique ID of the credential that is automatically generated by the connector. This is the Key Field and needs to be mapped to an Attribute on Select Identity and a dummy value needs to be passed while adding the user. This value will not be used by connector.
Credential UserID*	userID	The user's account for this credential.

Table 6 Citrix Mapping Information (cont'd)

Select Identity Resource Attribute	Citrix Password Manager Attribute	Description
Credential Password*	password	The user's password for this credential.
CustomField1	CustomField1	The custom values for this credential. This can be something like 'Domain name' needed along with user account information (userid/password). To know if the credential requires a custom field, refer the 'Application definition'.
CustomField2	CustomField2	The second custom field value for the credential.

After mapping the attributes, you can use the connector to create a service, or you can associate the connector with an existing service. Refer to the *Service Studio* chapter of the *HP Select Identity Administration Online Help* for information on Select Identity services.

5 Uninstalling the Connector

If you want to uninstall a connector from Select Identity, perform the following steps:

- Remove all resource dependencies.
- Delete the connector from Select Identity.
- Delete the connector from application server.

See *HP Select Identity Connector Deployment Guide* for more information on deleting the connector from application server and Select Identity.

A Sample Deployment Scenario

Citrix connector provisions secondary credentials to end users. The unique identifier for each end user is its fully qualified domain name (FQDN). The FQDN is used as an attribute while provisioning the credentials. This end user can be created through Select Identity or the end user maybe existing and the FQDN value is used while provisioning.

The example deployment scenario has the following environment:

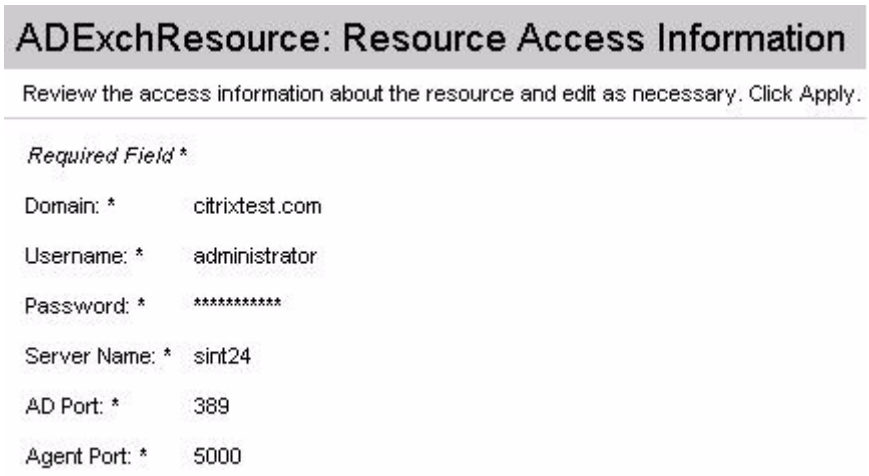
- Citrix Password Manager 4.1 on Windows 2003 installed with Active Directory 2003 as Central Store.
- Citrix connector v1.0 deployed on Select Identity 4.0.

These are two sample scenarios and the Citrix connector does not mandate the usage of the Active Directory connector or any other connector with it.

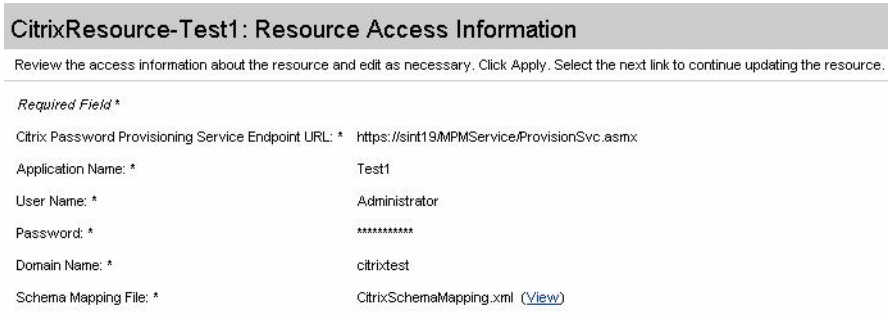
Scenario A

The end user is created from Select Identity using another connector. This user is then provisioned secondary credentials for various application definitions as additional services for the base user. The end user is the identity on Select Identity and secondary credentials as the associated services with the user's primary service.

1 The Active Directory connector is deployed and configured on Select Identity. This Active Directory connector is capable of provisioning users to the Active Directory central store of Citrix Password Manager.



2 The Citrix connector is deployed and configured on Select Identity. The Citrix resource is capable of provisioning secondary credentials to an Existing Application Definition on Citrix Password Manager called 'Test1'



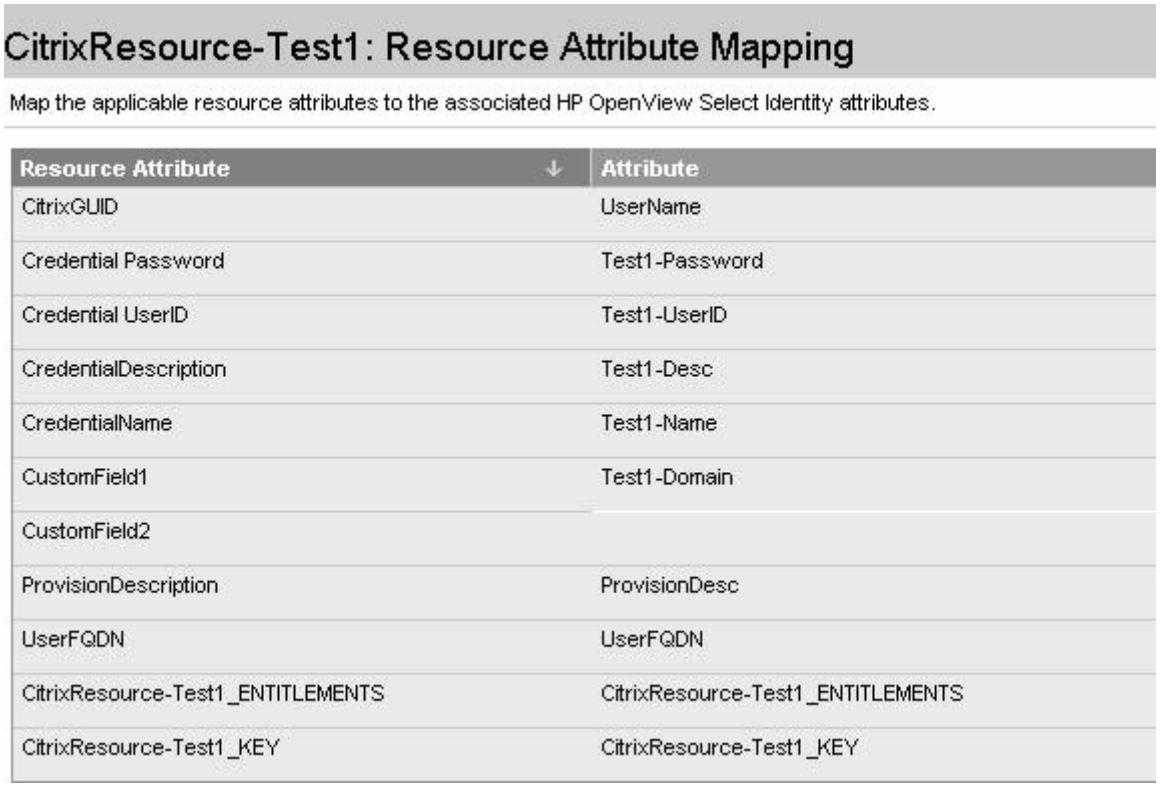
CitrixResource-Test1: Resource Access Information

Review the access information about the resource and edit as necessary. Click Apply. Select the next link to continue updating the resource.

Required Field *

Citrix Password Provisioning Service Endpoint URL: *	https://sint19/MPMService/ProvisionSvc.asmx
Application Name: *	Test1
User Name: *	Administrator
Password: *	**********
Domain Name: *	citrixtest
Schema Mapping File: *	CitrixSchemaMapping.xml (View)

3 Relevant attributes for the Citrix Resource of Test1 are created on Select Identity and mapped to the schema mapping file attributes. The `CitrixGUID` is the key field but its value is auto-generated by Citrix Password Manager. So this value is automatically set by the connector during add operation. This attribute just needs to be mapped and provided a dummy value. Below, the attribute is mapped to `UserName` attribute of Select Identity.



CitrixResource-Test1: Resource Attribute Mapping

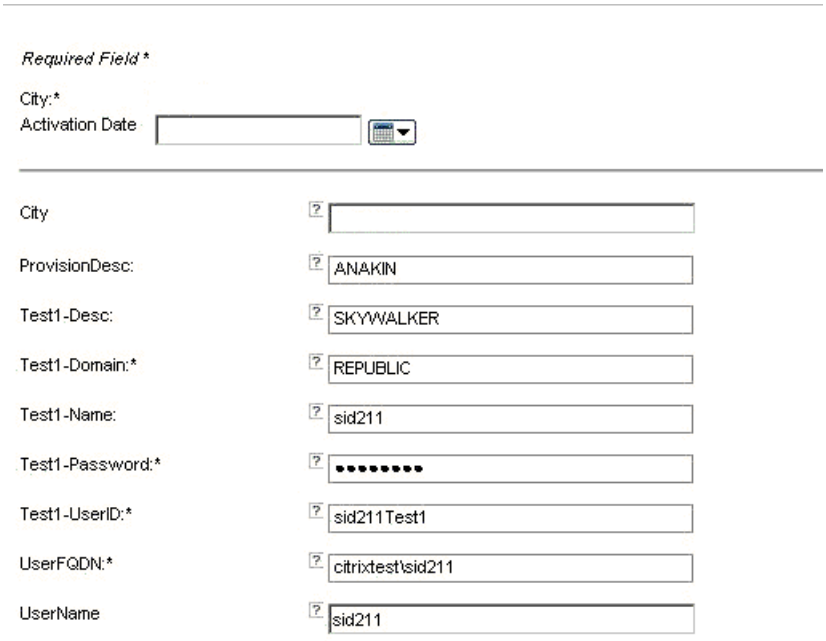
Map the applicable resource attributes to the associated HP OpenView Select Identity attributes.

Resource Attribute ↓	Attribute
CitrixGUID	UserName
Credential Password	Test1-Password
Credential UserID	Test1-UserID
CredentialDescription	Test1-Desc
CredentialName	Test1-Name
CustomField1	Test1-Domain
CustomField2	
ProvisionDescription	ProvisionDesc
UserFQDN	UserFQDN
CitrixResource-Test1_ENTITLEMENTS	CitrixResource-Test1_ENTITLEMENTS
CitrixResource-Test1_KEY	CitrixResource-Test1_KEY

4 Select Identity Services for Active Directory resource and Citrix resource are created.

5 The end user is created using the Active Directory connector. This is the user to which you can provision secondary credentials. The FQDN of this user will be used as a required attribute by Citrix connector.

6 Perform Subscribe to Service… for the user created above. Select CitrixService-Test1. Provide the relevant data for provisioning the secondary credential for the end user for the Application Definition 'Test1'.



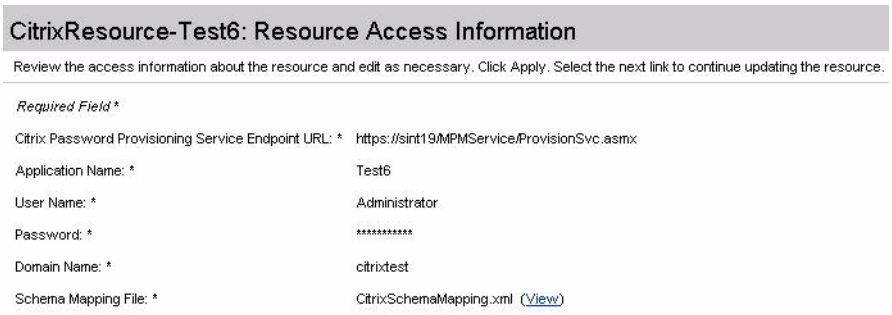
7 The end user now has the secondary credential for 'Test1' application definition provisioned. This can be verified by re-starting the 'Password Manager Agent'.

8 For provisioning secondary credentials for multiple Application Definitions for an end user, Select Identity Resources should be created and configured for each application definition on Citrix Password Manager (as in step 3 for Test1 application definition). Each such Resource can be associated with services and the 'Subscribe to Service…' operation can be used to provision the secondary credential for that Application definition.

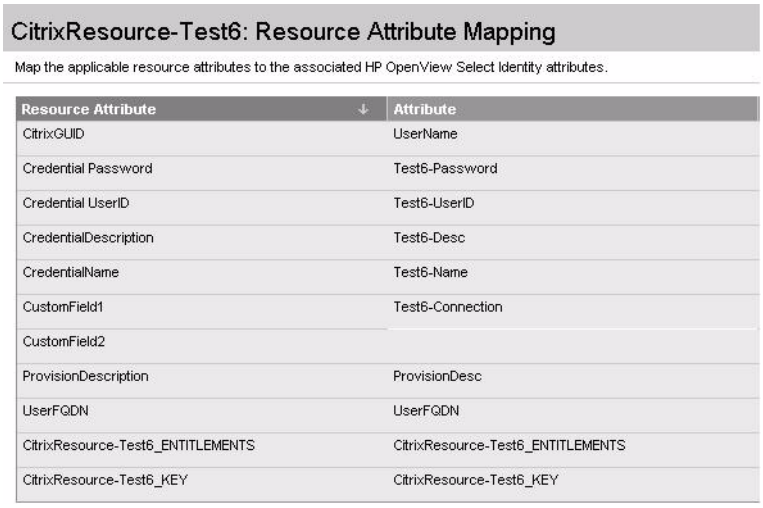
Scenario B

The end user already exists on the domain. The FQDN of this user is then used to provision secondary credentials for various application definitions as identities on Select Identity. That is, each secondary credential is the identity on Select Identity created by an add operation.

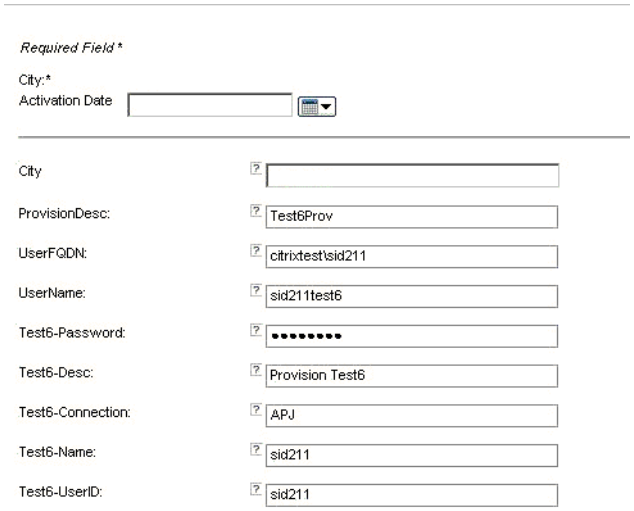
1. The Secondary credential is recognized as an identity on Select Identity.
2. The Citrix Connector is deployed and configured on Select Identity. The Citrix resource is capable of provisioning secondary credentials to an Existing Application Definition on Citrix Password Manager called 'Test6'.



3. Relevant attributes for the Citrix Resource of Test6 are created on Select Identity and mapped to the schema mapping file attributes. The `CitrixGUID` is the key filed but its value is auto-generated by Citrix Password Manager. So this value is automatically set by the connector during add operation. This attribute just needs to be mapped and provided a dummy value. Below, the attribute is mapped to `UserName` attribute of Select Identity.



4. Select Identity Services Citrix Resource is created.
5. Perform 'Create User' for the above Resource and provide relevant values.



6 The secondary credential is provisioned and is an identity on Select Identity referred by the value for 'UserName' provided.